Exhibit C

azcentral.

ELECTIONS

Election experts say giving Maricopa County routers to Arizona Senate's election auditors could be security threat

Jen Fifield Arizona Republic

Published 1:54 p.m. MT May 11, 2021 | **Updated 5:48 p.m. MT May 11, 2021**

Routers serve as the mail carrier of a computer network: They deliver messages using maps of networks and computer addresses.

Think of it like a mail carrier who relies on maps and addresses to get mail to the right place.

Given access to the mail carriers' — or routers' — information, it would be easier for a bad actor to get access to a person's mail, or to target the information inside the network.

That's an analogy one tech expert – Matt Bernhard, a research engineer at Voting Works, a nonpartisan nonprofit that advocates for open source election technology — gave while explaining the importance of keeping Maricopa County's routers secure.

Arizona Senate Republicans are trying to get access to the county's routers and administrative passwords to the county's voting machines, and to provide that to private contractors they've hired to audit the county's 2020 election results, which began April 23.

Bernhard said providing access to the routers is a "pretty specific risk" to the county. Also, he and other election security consultants across the country are unsure why exactly the auditors would need the routers to audit the election results.

Senate liaison Ken Bennett has said they are needed to check whether the county's voting machines were connected to the internet during the election. But a county spokesperson said that the auditors already have the information and machines to perform that check, and a previous independent audit commissioned by the county proved they were not.

County Attorney Allister Adel has said that giving access to the routers would risk county residents' Social Security information and public health information, along with sensitive law enforcement data.

Bernhard and others said it would be odd to find that information on a router, but said, given the information that is on the routers, it might be easier for someone to hack into the county's network to get it.

Meanwhile, an attorney for Senate Republican leaders has dismissed this idea and threatened to file another subpoena to haul the county Board of Supervisors before the state Senate to explain why they won't cough up the routers.

Why do auditors need the routers?

Senate Republicans in January issued subpoenas to the county requesting not only all 2.1 million ballots cast in the county's general election, all of the county's voting machines and the county's voter rolls but also "access or control of ALL routers, tabulators or combinations thereof, used in connection with the administration of the 2020 election, and the public IP of the router."

Cyber Ninjas, the main contractor hired by the Senate to oversee the audit despite having no experience leading election audits, said in its original work plan that it would inspect the county's voting systems in many ways, but offers nothing specific about examining routers.

One item says that the contractors will attempt to identify "usage of cellular modems, Wi-Fi cards, or other technologies that could be utilized to connect systems to the internet or wider-area-network."

Bennett said he believes the contractors want the routers to address concerns from "people that have always suspected something nefarious about elections being connected to the internet."

But Megan Gilbertson, spokesperson for the county Elections Department, has reiterated that the county's ballot-counting machines are not connected to the internet. She said the county has provided the contractors with what they need to confirm that.

"In January, the county provided Windows event logs, precinct-based tabulator logs, Election Management System workstations, server logs and more in compliance with the Senate's subpoena," Gilbertson said. "Someone with knowledge of the equipment would be able to confirm through a review of those logs that the equipment was not connected to the internet."

Also, independent contractors hired by the county already checked for that in a previous audit. The results from that audit found no malicious hardware on voting machines, found

that the machines were not connected to the internet, and found that the machines were programmed to tabulate ballots accurately.

Nicholas Weaver, a network security researcher at the International Computer Science Institute and computer science lecturer at University of California, Berkeley, said that the router might have logs about internet access different from what's seen on a server or the voting machines. But they could probably still thoroughly check whether the machines were connected to the internet without the routers, Weaver said.

Providing the routers would be disruptive to county business, since the county would need to take the routers offline to make a forensic copy, and get other routers to provide the network service in the interim, he said.

"What the (routers) would provide the state recounters is absolutely nothing other than making life completely miserable for those providing the data," Weaver said.

County Supervisors Chairman Jack Sellers said last week that it would cost as much as $6 million if the county has to replace the routers while the Cyber Ninjas has them.

Pursuit of routers raises concerns for some IT consultants

Many election security consultants told The Republic they are concerned by the demand.

The routers aren't needed to audit election results, and the lack of clear answers about why the Senate's contractors want them raises questions, said Matt Masterson, former head of election security at the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency,

He said when voting systems are tested at the federal level, there is typically:

- Full transparency about the standards used to test the equipment.
- Details about how the equipment will be tested.
- Information about what will be included in the final report.

The private contractors haven't provided that clarity.

“The request leaves those who understand these systems and processes with their hand up in the air saying, 'What are you doing? What are you trying to do?” Masterson said.

Weaver said there is "no logic" in the demands.

"It is a 100% malicious request," he said, referring to the inconvenience and potential risk to the county with no clear benefit.

For subscribers: After 2 weeks of counting, election experts warn of harmful effects from Arizona election audit

What routers did the Senate demand?

Routers are hardware that connect local networks to the internet or to other networks.

There are many different types, including simple routers used at home to connect computers and smartphones to the internet, as well as complex commercial routers that can be programmed to store logs of activity and data and protect from outside intruders, Bernhard said.

The routers demanded in the January subpoenas route network traffic across 50 different county departments, not just the Elections Department, said county spokesperson Fields Moseley.

Some county routers aren't connected to the internet and are used to route internal network information, such as case management files or public health information, he said. Others are connected to the internet and are "specialty routers that have a significant level of security and are sized to handle a high level of network traffic," Moseley said.

What information is stored on the routers?

County IT experts say that a router is like a switchboard in that it shows how the county's entire network is laid out, Moseley said.

"If you have access to the router, you potentially have the IP 'blueprints' for the entire county, giving a hacker the ability to infiltrate or intercept confidential and sensitive information on the county network," he said.

Generally, some routers retain logs about internet connections and searches, said Alex Halderman, a University of Michigan computer science and engineering professor who specializes in election security. There may also be information about virtual private networks, or VPNs, and firewall configurations.

All of that information could be useful information for someone who wanted to try to hack into a system, Halderman said.

Bernhard said it could be that the data would reveal IP addresses of confidential computers or servers where law enforcement is storing data and how that data is protected, for example.

But it's unlikely that the logs would give detailed information about the actual information on the county's internet or networks, Bernhard said.

Back to Bernhard's mail carrier analogy, the carrier takes your information and sends it somewhere else but doesn't open it up to see what's inside.

If the carrier was to look inside, in this example it's likely the messaging would be gibberish. That's because the county is probably encrypting its data in some way.

'Arizona is playing a dangerous game': John Oliver gets serious about election audit

What passwords do the Senate contractors still want and why?

The Senate's second demand is for passwords to the county's ballot tabulators used on Election Day at voting centers.

The private contractors conducting the audit returned most of the county's machines after pulling data from them, but hung onto the vote center tabulators.

The password and security tokens the state Senate wants provides administrative access to Dominion Voting Systems' proprietary firmware and source code, Sellers said.

The county does not have that administrative access, Sellers said.

Dominion Voting Systems, which leases the voting machines to the county, has that information, Gilbertson said.

But it's not clear what the auditors could see with the administrative access.

Masterson said it's unlikely that the source code is kept on the machines, considering there is a requirement within federal standards for voting systems that source code is not kept that way. Bernhard agreed that it's unlikely the source code is on the machine.

Auditors could look at the hash coding of the machine to see that it is still the same as when it was provided to the county, Masterson said.

It's unclear whether the auditors have the access or information to do that without the administrative passwords.

Typically when you look at a machine's firmware, Bernhard said, you compare it to something else to see whether it has changed. He isn't sure the auditors have anything to compare what they are looking at with, and reverse engineering it would take a lot of time.

During the county's independent audit, the companies were able to compare the hash coding of the machines to the original, perhaps because they are accredited by the U.S. Election Assistance Commission to certify voting machines and have that information available.

Examining the machines' firmware is generally a way to analyze the system vulnerabilities by looking where the holes in security are, Halderman said.

"It's quite concerning if information about the technical specifics of security flaws in voting machines falls into the wrong hands," he said.

For subscribers: Arizona Republicans worry about consequences from election audit: 'This is turning into a mockery'

What will this mean for elections here and elsewhere?

Handing the routers and passwords over to untrusted parties "might create very real risks" for the county, Halderman said.

County officials were not present when the auditors made virtual copies of the machines and the process was not open to all observers or livestreamed online.

Halderman said he found it "pretty remarkable," that the machines were left with private contractors, unmonitored by election officials. Bad actors could have tampered with the machines during that time, he said.

Halderman said auditors also could use what they learned about the machines to try tohack into these machines or similar machines elsewhere, he said.

Bernhard said if the auditors get access to the sensitive information, he is more concerned about the precedent that sets than the actual event. All of this, he said, could lead to more claims of election fraud and more distrust in the system.

"It's not going to be a good thing for democracy in the U.S. as a whole," he said.

Reach the reporter at jen.fifield@azcentral.com or at 602-444-8763. Follow her on Twitter @JenAFifield.

Hyperlink inoperable on pdf, full hyperlink below:

https://www.azcentral.com/story/news/politics/elections/2021/05/11/experts-say-giving-maricopa-county-routers-arizona-senates-election-auditors-bad-precedent/4995728001/